## REMARKS

Claims 1-47 are pending in this application. Claims 1-19, 27 and 41 are canceled without prejudice. Thus, claims 20-26, 28-40, and 42- 47 are pending and at issue.

## 35 U.S.C. § 112

Applicants respectfully traverse the rejection of claims 25 and 39 under 35 U.S.C. § 112 for lacking antecedent basis for the term "back-off." Regarding antecedent basis in the claims, claims 25 and 39 specifically recite "a random back-off," and thus, does not require antecedent support. Moreover, the specification discusses and supports the element of a member having random back-off prior to processing a renewal request at least at paragraph 0057. Applicants submit that the term "back-off" is well known to those skilled in the art, and specifically refers to a period of time in which a device does not attempt to process a communication request. However, applicants have amended claims 25 and 39 to recite a random back-off period to more clearly indicate that the back-off is a period. Applicants submit that claims 25 and 39 are allowable under 35 U.S.C. § 112.

Applicants respectfully traverse the rejection of claims 31 and 45 under 35 U.S.C. § 112 for lacking antecedent basis for the term "deprecate." Regarding antecedent basis in the claims, claims 31 and 45 specifically use "deprecate" as a verb. Specifically, claims 31 and 45 recite that administrator privileges are first deprecated prior to publishing a revocation record. There is no antecedent support required. Moreover, the specification discusses and supports that administrator privileges are first deprecated prior to publishing a revocation record at least at paragraph 0071 and 0078. Furthermore, as described in paragraph 0078, deprecation is a notification mechanism which allows all the members who have been issued a certificate by the revoked administrator to realize that the administrator is about to be revoked. Also, as known by those skilled in the art, a deprecated function is a function that is being phased out. Applicants submit that claims 31 and 45 are allowable under 35 U.S.C. § 112.

## 35 U.S.C. § 102

Applicants respectfully traverse the rejection of claims 26, 28, 40, and 42 as anticipated by Yeager et al. Claim 26 is amended to recite the limitation of claim 27 and

claim 40 is amended to recite the limitation of claim 41. Claims 27 and 41 are canceled. Each of the claims 26, 28, 40, and 42 now recites creating a token for a publisher where the token is published in a graph database and where the graph database provides security related information including the published token to each member of the secure group. Yeager et al. fails to disclose publishing a token to a graph database that provides security related information to each member of the group. Instead, at cited paragraph 0256, Yeager et al. merely describes that a peer member is capable of caching information. If the office action is indicating that the peer cache is a database, then Yeager et al. still fails to disclose that a token is published to the cache, or that security information is provided to each member of the group from the cache. It follows that Yeager et al. fails to disclose publishing a token to a database that provides security information to each member of a group. Therefore, Yeager et al. cannot anticipate claims 26 and 28 and 40 and 42.

Applicants respectfully traverse the rejection of claims 29-31 and 43-45 as anticipated by Yeager et al. Each of claims 29-31 and 43-45 recites publishing a revocation record to a group where the revocation record identifies a member of a group and revoking any records published by the member according to the revocation record. While Yeager et al. discloses at paragraph 0058 the general concept in which a member of a group can be revoked, Yeager et al. fails to disclose or teach how revocation is implemented. Specifically, in relation to the pending claims, Yeager et al. fails to disclose a revocation record, much less publishing a revocation record to a group and revoking any records of an identified member of the revocation record based on the revocation record. Therefore, Yeager et al. can not anticipated claims 29-31 and 43-45.

## 35 U.S.C. § 103

### A.    Yeager et al. in view of Yellepeddy et al.

Applicants respectfully traverse the rejection of claims 20-21 and 34-35 as obvious over Yeager et al. in view of Yellepeddy et al. Each of claims 20-21 and 34-35 is amended to recite receiving a certificate renewal request at a second member in the group from a first member, requesting by the second member authorization from an administrator for renewing the certificate, and renewing the certificate based on authorization from an administrator or security policies. As acknowledged by the office action, Yeager et al. fails to disclose

renewing a certificate in any manner. Instead, the office action relies on Yellepeddy et al. to remedy the deficiency. Unfortunately, while Yellepeddy et al. discloses a process of renewing a certificate, Yellepeddy et al. still fails to disclose the recited certificate renewal process. Specifically, Yellepeddy et al. fails to disclose renewing a first member certificate by receiving a renewal request at a second member, where the second member requests authorization from an administrator for renewing the certificate. Generally, the claimed renewal process of claims 20-21 and 34-35 is implemented in a peer to peer network in which one peer acts on behalf of another peer to initiate a renewal process. Yellepeddy et al. is primarily concerned with providing a system in which the workload of certificate renewal by a certificate authority may be distributed among other certificate authorities that share a common public certificate. In fact, the cited paragraph 0092 of Yellepeddy et al. merely discloses a process in which the multiple certificate authorities update their shared public certificate so that none of certificate authorities have an expired public certificate (which would make a certificate authority inoperative). Yellepeddy et al. does not teach a second peer member acting on behalf of a first peer member to initiate a renewal process after receiving a renewal request from the first peer. Thus, neither Yeager et al. nor Yellepeddy et al. disclose the recited element. It follows, therefore, that no combination of Yeager et al. and Yellpedy et al. can render claims 20-21 and 34-35 obvious.

Applicants respectfully traverse the rejection of claims 22-25 and 36-39 as obvious over Yeager et al. in view of Yellepeddy et al. Each of claims 22-25 and 36-39 recite receiving a request to renew a certificate that is published in a graph database and performing renewal according to an authorization from an administrator or based on one or more security policies. Neither Yeager et al. nor Yellepeddy et al. disclose publishing a certificate in a graph database, and thus, no combination of Yeager et al. and Yellepeddy et al. can render claims 22-25 and 36-39 obvious.

While Yeager et al. discloses the ability to publish records at paragraph 0223 and the ability to renew a group membership at paragraph 0225, Yeager et al. fails to disclose publishing a certificate in a graph database. Yellepeddy et al. also fails to disclose publishing a certificate in a graph database. In fact, Yellepeddy et al. fails to disclose a database shared by a graph or interconnection of nodes. It follows, therefore, that no combination of Yeager et al. and Yellepeddy et al. can render claims 22-25 and 36-39 obvious.

**B.     Yeager et al. in view of Aguilera et al.**

Applicants respectfully traverse the rejection of claims 32, 33, 46, and 47 as obvious over Yeager et al. in view of Aguilera et al. (U.S. Publication No. 2004/0243827). Each of claims 32, 33, 46, and 47 recite a revocation bit map comprising one or more bits that identify one or more members of a group and altering one or more bits of the revocation bit map to revoke one or more members of the group. Neither Yeager et al. nor Aguilera et al. disclose or teach a revocation bit map having bits that identify members of a group and altering one or more bits of the revocation bit map to revoke one or more members of a group. Therefore, no combination of Yeager et al. and Aguilera et al. can render claims 32, 33, 46, and 47 obvious.

As acknowledged by the office action, Yeager et al. fails to disclose using a bit map to revoke a member of a group. Instead, the office action relies on Aguilera et al. to remedy the deficiency. However, Aguilera et al. also fails to disclose the recited revocation bit map or altering a revocation bit map to revoke members of a group. Generally, Aguilera et al. discloses using a capabilities revocation list and a group list containing a list of valid groups corresponding to granted capabilities (both of which may be in bitmap form) to determine whether a client has the right or privilege to execute a function (such as a request to access data). See paragraph 0004 and 0013. Aguilera et al. further discloses that if a client is requesting execution of a function that is on the capabilities revocation list, then the client will be unable to execute the function. Aguilera et al. also discloses that a capability may be revoked for a group having the capability by invalidating the group in the group list. Neither one of these lists, however, list elements that correspond to individual members of a group. At best, the Aguilera et al. revocation list and its corresponding capabilities group list teach parameters that may be associated with a member of a group. Because neither of the Aguilera lists contain elements that correspond to members of a group, no alteration of the bits of a bitmap derived from the Aguilera lists can result in revoking members of a group. It follows, therefore, that no combination of Yeager et al. and Aguilera et al. can render claims 32, 33, 46, and 47 obvious.